UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/560,177	01/29/2007	Arthur D. Kranzley	070457.2081	1386

21003 7590 01/09/2009

BAKER BOTTS L.L.P.
30 ROCKEFELLER PLAZA
44TH FLOOR
NEW YORK, NY 10112-4498

EXAMINER	
KAMAL, SHAHID	

ART UNIT	PAPER NUMBER
3621	

NOTIFICATION DATE	DELIVERY MODE
01/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DLNYDOCKET@BAKERBOTTS.COM

Office Action Summary	**Application No.** 10/560,177	**Applicant(s)** KRANZLEY ET AL.
	Examiner SHAHID KAMAL	**Art Unit** 3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _09 December 2005_.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-22_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)□ Claim(s) _____ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _08/24/2006_.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Acknowledgements

1. The claims 1-22 are currently pending and have been examined.

2. This Office Action is response to the application filed on December 09, 2005.

Information Disclosure Statement

3. The Information Disclosure Statement filed on 24 August 2006 has been considered. An initialed copy of the Form 1449 is enclosed herewith.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-22 are rejected under 35 U.S.C. 102(e) as anticipated by Hogan et al. (US Patent No. 6,915,279 B2) ("Hogan").

Referring to claim 1, Hogan discloses the following:

a) an issuer (issuer 406) platform layer including at least one 3-D Secure authentication program (authentication data 414) (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67);

b) a merchant (merchant 404) plug-in (MPI)(see abstract, figures 1, 2, column 1, lines 37-61, column 4, table I, column 3, lines 27-58, column 11, lines 1-58, column 20, lines 19-67);

c) an secure payment algorithm (SPA) (see column 6, lines 1-18, table II, column 7, lines 1-18, column 9, lines 51-67, column 24, lines 51-67); and

d) a data transport layer, wherein the issuer (issuer 406) platform comprises an access control server (ACS) that uses the SPA to process transaction and cardholder information for authentication by an authentication method and to generate an Accountholder Authentication Value (AAV) and conveys the AAV through the data transport layer to the MPI, wherein the AAV is a formatted data structure compatible with 3-D Secure message protocols, wherein the formatted data structure has a length of at most 20-bytes including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that identify secret cryptographic keys and bytes that include a merchant authentication code (MAC) (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67).

Referring to claim 2, Hogan discloses wherein the AAV is a formatted data structure that is Base 64 encoded (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67).

Referring to claim 3, Hogan discloses wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and a plurality of the fields of the bytes 6fthe AAV excluding bytes that represent the MAC, and wherein a portion of the encryption result forms the MAC bytes in the 25 AAV (see abstract, column 6, lines 1-18, table II, column 7, lines 1-18, column 9, lines 51-67, column 24, lines 51-67).

Referring to claim 4, Hogan discloses wherein the SPA comprises an encryption algorithm for generating the MAC, wherein the encryption algorithm uses a pair of secret keys A and B that are identified in the AAV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a 30 three-digit CVC2 field, and uses the result to populate two bytes of the MAC (see abstract, column 6, lines 1-18, table II, column 7, lines 1-18, column 9, lines 51-67, column 24, lines 51-67).

Referring to claim 5, Hogan discloses wherein the pair of secret keys A and B are 64- bit Data Encryption Standard (DES) keys (see abstract, column 6, lines 1-18, table II, column 7, lines 1-18, column 9, lines 51-67, column 24, lines 51-67).

Referring to claim 6, Hogan discloses wherein the ACS is configured to generate an AAV in response to a payment authentication request message from the MPI to the ACS (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 7, Hogan discloses which is configured to transport the A.AV in a payment authentication response message from the ACS (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 8, Hogan discloses wherein the ACS is further configured to place a digital signature on the payment authentication response message (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 9, Hogan discloses wherein the MPI is configured to verify the digital signature on a received payment authentication response message (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 10, Hogan discloses wherein the MPI is configured to extract the MAC fields included in a payment authentication response message from the ACS and to place the extracted MAC in a payment authorization request message to a third party (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 11, Hogan discloses a data structure for conveying cardholder transaction authentication information amongst stakeholders in a 3-D Secure environment, the data structure comprising 20 bytes of Base 64 encoded characters, wherein the first byte is a control byte, bytes

2-9 represent a hash of a merchant name, byte 10 identifies an Access control server (ACS) that authenticates the cardholder transaction by an authentication method, byte 11 identifies the authentication method and the secret encryption keys that are used by the ACS to generate a Merchant Authentication 'Code (I~AC), bytes 12- 15 represent a transaction sequence number identifying a transaction number processed by the ACS, and bytes 16-20 represent the MAC (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 12, Hogan discloses wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number and a plurality of the fields of bytes 1-15 of the data structure, and wherein a single key identified in byte 11 is used for encryption (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 13, Hogan discloses wherein the MAC comprises portions of an encryption of a concatenation of the card holder's account number, card expiration date and service code, and wherein a pair of keys A and B that are identified in byte 11 is used for encryption (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 14, Hogan discloses wherein a three-digit encryption result is used to populate two bytes of the MAC bytes 16-20 (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 15, Hogan discloses wherein the pair of secret keys A and B are 64 bit Data Encryption Standard (DES) keys (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 16, Hogan discloses the following:

a) using an Access control server (ACS) to process cardholder and transaction information to authenticate the cardholder by an authentication method (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67);

b) deploying a secure payment algorithm (SPA) to generate an Accountholder Authentication Value (AAV) to represent the authentication results, and transporting the AAV in 3-D Secure messages to the merchant, wherein the AAV is a formatted data structure that has a length of at most 20 bytes, including bytes that identify a hash of the merchant's name, bytes that identify the ACS, bytes that identify the authentication method, bytes that include a merchant authentication code (MAC), and bytes that identify secret cryptographic keys that are used by the

SPA to generate MAC (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67).

Referring to claim 17, Hogan discloses wherein the AAV is a formatted data structure that is Base 64 encoded (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67).

Referring to claim 18, Hogan discloses using a secret key identified in the AAV to encrypt a concatenation of the card holder's account number and at least portions of the bytes of the AAV 25 excluding bytes that represent the MAC (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67); and assigning a portion of the encryption result to the MAC bytes in the AAV (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 19, Hogan discloses using a pair of pair secret keys A and B that are identified in the A.AV to encrypt a concatenation of the card holder's account number, card expiration date and service code to generate a three-digit CVC2 field (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67); and assigning the result to populate two bytes of the MAC (see abstract, figures 1,9, 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 11, lines 30-58, column 24, lines 1-67).

Referring to claim 20, Hogan discloses wherein the pair of secret keys A and B are 64 bit Data Encryption Standard (DES) keys (see abstract, column 6, lines 1-18, table II, column 7, lines 1-18, column 9, lines 51-67, column 24, lines 51-67).

Referring to claim 21, Hogan discloses wherein transporting the AAV in 3-D Secure messages to the merchant, comprises transporting the AAV in a payment authentication response message that is digitally signed by the ACS (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Referring to claim 22, Hogan discloses first, verification by the merchant of the digital signature on a received payment authentication response message (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67); and next, extraction of the MAC fields from the received payment authentication response message by the merchant (see abstract, figures 2, 6, column 1, lines 37-61, column 2, lines 1-37, column 3, lines 27-58, column 6, lines 1-18, column 14, lines 4-64, column 21, lines 1-35, column 22, lines 53-67).

Examiner's Note:

6. The Examiner has pointed out particular references contained in the prior art of record within the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the entire reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the Examiner.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication or earlier communications from the patent examiner should be directed to Shahid Kamal whose telephone number is (571) 270-3272. The Patent examiner can normally be reached on Monday-Thursday (9:00am -7:00pm), Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew J. Fischer can be reached on (571) 272-6779. The fax phone number for this origination where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published application may be obtained from either Private PAIR or Public PAIR.

Statues information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-directed.uspto.gov.

Should you have any questions on accessing to the Private PAIR system, contact the Electronic Business Center (EBC) at 1(866) 217-9197 (toll free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 1(800) 786-9199 (IN USA OR CANADA) or 1(571) 272-1000.

Shahid Kamal
January 3, 2009

/EVENS J. AUGUSTIN/
Primary Examiner, Art Unit 3621